Как распознать мошенничество?

Телефонные мошенничества

Как распознать мошенника?

Вам поступает звонок якобы сотрудника правоохранительных органов (ФСБ, СК, прокуратура, полиция);

Вам сообщают, что кто-то из близких попал в ДТП, больницу, совершил преступление, и ему срочно нужны деньги;

Поступает звонок или СМС от якобы сотрудника службы безопасности банка;

Вы получаете СМС или звонящий сам сообщает, что вы стали обладателем приза или победителем конкурса;

Затем просят сообщить реквизиты карты и ваши персональные данные, перечислить деньги на безопасный счет, оформить кредит, пока на вас его не оформили злоумышленники и т.д.

Телефонные мошенничества

Что делать?

Позвоните своему близкому человеку, в больницу, в органы внутренних дел **проверьте информацию;**

Никогда **не передавайте и не переводите деньги** незнакомым людям. Не верьте в **безопасный счет – это уловки**. Банк никогда не попросит Вас перевести куда-то деньги, назвать CVV/ CVC-код или код и смс.

Кибермошенничество

Как распознать мошенника?

На Ваш смартфон или компьютер поступает сообщение либо письмо с любой информацией с ссылкой, по которой необходимо перейти (призывы проголосовать в конкурсе, получить в подарок бесплатную подписку на какой-либо сервис и т.д.);

Вы сами устанавливаете на свой смартфон или компьютер не лицензионное программное обеспечение. При этом не обращаете внимание, что предоставляете этой программе доступ к сети интернет, отправке СМС и т.д.;

Если вы теряете свой мобильный телефон с подключенной услугой «Мобильный банк», его может найти мошенник.

Кибермошенничество

Что делать?

Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие по СМС, ММС, электронной почте, мессенджерам, в том числе от имени банков;

Установите на телефон и на вход в «Мобильный банк» **надежные пароли**;

Если Вы потеряли телефон, позвоните в банк или **заблокируйте карты** через сервис «Интернет банк».

Мошенничества в сети интернет

Как распознать мошенника?

Реклама биржевых площадок с крупными заработками в короткие сроки. После перечисления средств вы не сможете вернуть их обратно, и виртуальные заработки на бирже так и останутся виртуальными.

Сайты-клоны торговых площадок с отличной репутацией (копируют интерфейс оригинального сайта), с небольшим отличием в доменном имени сайта.

Мошеннические интернет-магазины с товарами по цене существенно ниже среднерыночной либо с большими скидками.

На ваше объявление о продаже товара звонит мошенник с намерением купить ваш товар, но просит сообщить данные вашей банковской карты для перевода на нее денежных средств или оплатить через сторонний сервис по ссылке.

Мошенничества в сети интернет

Что делать?

Проверьте, правильно ли Вы написали **доменное имя сайта**. Зайдите в раздел сайта, где размещены **контактные данные сайта**. Если указан лишь адрес электронной почты или телефон, воздержитесь от покупки;

Никому **не сообщайте** данные своей банковской карты, **CVV/ CVC-код или код и смс**.
Для перевода средств достаточно только номера карты и имени держателя карты (без фамилии);

Относитесь с осторожностью
к предложениям получения прибыли
в короткие сроки.